WHAT IS CLAIMED IS:

1. A method for encrypting and decrypting contents data to be distributed from a server to a user terminal through a network, said method comprising:

generating a first key at the server from contents information about the distributed contents data;

generating a second key at the server from a variable parameter, a H/W key ID, and said first key and sending the generated second key to the user terminal;

decrypting the first key at the user terminal from the variable parameter, the H/W key ID, and said second key;

encrypting the contents data to be distributed at the server by using said first key and sending the encrypted contents data to the user terminal; and

decrypting the encrypted contents data at the user terminal by using said decrypted first key.

2. The method according to claim 1, the method further comprising generating the variable parameter at the user terminal and sending the generated variable parameter to the server.

3. The method according to claim 2, wherein the variable parameter used for generating the second key at the server are the variable parameter sent from the user terminal.

4. The method according to claim 1, the method

further comprising synchronizing the variable parameter between the user terminal and the server.

5. The method according to claim 4, wherein said synchronization between the user terminal and the server is performed at a time different from a time when the contents data is distributed.

6. A contents data encrypting and decrypting system comprising:

a server,

the server comprising;

means for generating a first key from contents information of contents data to be distributed,

means for generating a second key from a variable parameter, a H/W key ID, and said first key, and

means for encrypting the contents data to be distributed by using the first key; and

a user terminal,

the user terminal comprising;

a network interface configured to receive said second key and said encrypted contents data from said server,

means for decrypting the first key from the variable parameter, the H/W key ID, and said second key, and

means for decrypting said encrypted contents

data by using said decrypted first key.

7. The contents data encrypting and decrypting system according to claim 6, the system further comprising

means for synchronizing the variable parameter between said server and said user terminal.

8. A user terminal used for encrypting and decrypting contents data to be distributed from a server through a network, the user terminal comprising:

a network interface configured to receive from the server a second key generated from a first key generated from contents information of the contents data to be distributed, a variable parameter, and a H/W key ID, and the contents data encrypted by using said first key; and

a decrypting section configured to decrypt the first key from the variable parameter, the H/W key ID, and said second key, and then decrypt said encrypted contents data by using said decrypted first key.

9. The user terminal according to claim 5, the user terminal further comprising means for synchronizing the variable parameter between the server and the user terminal.